UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,139	07/25/2001	Allen Michael Salomon	54308-0012	8227

29989 7590 03/03/2005

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 03/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/916,139	SALOMON ET AL.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-23 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-3, 15-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Noll et al (U.S. 5,732,138) and further in view of Kaplan et al (U.S. 6,704,871).

As per claims 1, 15, 18, 21, Noll et al discloses a method used for encryption (see column 1 lines 33-34), the method comprising the steps of: receiving a first digital input from a set of possible digital inputs; wherein each digital input in said set of possible digital inputs to generate a corresponding unique output value; generating a first output value based on said first digital input; and generating a first encryption key based on the first output value (see column 4 lines 17-26 and column 3 lines 7-10).

Noll et al fails to disclose the generation being performed on an integrated circuit.

However, Kaplan et al teaches the use of an integrated circuit for such generation (see column 1 lines 38-41).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Kaplan et al's integrated circuit to perform the generation of Noll et al.

Motivation to do so would have made it possible to provide the generation in distributed computing (see Kaplan et al column 1 lines 42-43).

As per claims 2-3, 16-17, 19-20, 22-23, the modified Noll et al and Kaplan et al system discloses the step of generating a first output value is based on anomalies of said first integrated circuit wherein said anomalies are either inherit or intentionally induced (see Noll et al column 4 lines 17-26 where the hash function contains the anomalies).

4. Claims 4-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Noll et al and Kaplan et al system as applied to claim 1 above, and further in view of Matyas et al (U.S. 6,307,938).

As per claim 4, the modified Noll et al and Kaplan et al system fails to disclose generating a second output value based on applying a second digital input from a second integrated circuit; and the step of generating a first encryption key based on the first output value includes generating a first encryption key based the first output value and the second output value.

However, Matyas et al teaches such a technique (see column 6 lines 4-12 where the concatenation of the hash values is then sent to the key generator of Noll et al as above).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Matyas et al's method of applying a second output to a first for key generation.

Motivation to do so would have been to produce a bit string with a specified length (see Matyas et al column 6 lines 4-12).

As per claim 5, the modified Noll et al, Kaplan et al and Matyas et al system discloses the second digital input is generated based on said first output value (see Matyas et al column 6 lines 4-12).

5. Claims 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Noll et al and Kaplan et al system as applied to claim 1 above, and further in view of Ginter et al (U.S. 5,892,900).

As per claim 6, the modified Noll et al and Kaplan et al system fails to disclose generating a data structure that includes encrypted data.

However, Ginter et al teaches generating a data structure that includes encrypted data (see column 200 lines 1-14).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the modified Noll et al and Kaplan et al's key to encrypt the data of Ginter et al.

Motivation to do so would have been to protect the data.

As per claim 7, the modified Noll et al, Kaplan et al and Ginter et al system discloses causing said first digital input to be stored in persistent storage; causing said first digital input to be retrieved from said persistent storage; regenerating said first output value by causing said first digital input to be applied to said first integrated circuit; regenerating said first

encryption key based on said first output value; and decrypting said encrypted data using said first encryption key (see Ginter et al column 199 line 34 through column 200 line 14 as applied to the key generation above).

6. Claims 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Noll et al, Kaplan et al and Matyas et al system as applied to claim 4 above, and further in view of Ginter et al.

As per claim 8, the modified Noll et al and Kaplan et al system fails to disclose generating a data structure that includes encrypted data.

However, Ginter et al teaches generating a data structure that includes encrypted data (see column 200 lines 1-14).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the modified Noll et al and Kaplan et al's key to encrypt the data of Ginter et al.

Motivation to do so would have been to protect the data.

As per claim 9, the modified Noll et al, Kaplan et al, Matyas et al and Ginter et al system discloses causing said first digital input to be stored in persistent storage;

causing said first digital input to be retrieved from said persistent storage; causing said first digital input to be applied to said first integrated circuit to generate said first output value; regenerating said second digital input based on said first digital input; regenerating said second output value by applying said second digital input to said second integrated circuit; regenerating said first encryption key based on the second output value; and decrypting said encrypted data using said first encryption key (see Ginter et al column 199 line 34 through column 200 line 14 as applied to the key generation above).

7. Claims 10-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Noll et al, Kaplan et al, Matyas et al and Ginter et al system as applied to claims 1 and 6 above, and further in view of Belove et al (U.S. 5,115,504).

As per claim 10, the modified Noll et al, Kaplan et al, Matyas et al and Ginter et al system discloses generating a first data structure that contains first data and encrypted first data, wherein said encrypted first data is an encrypted version of said first data encrypted using said first encryption key (see Ginter et al as applied to claim 6 above), but fails to disclose causing to be stored

in persistent storage: a second data structure that specifies said first digital input, and linking data that associates said first data and said second data structure.

However, Belove et al teaches a second data structure that specifies said first digital input, and linking data that associates said first data and said second data structure (see column 1 lines 37-43).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Belove et al's method of linking in the modified Noll et al, Kaplan et al, Matyas et al and Ginter et al system.

Motivation to do so would have been have a pointer to a location of the linked data structures (see Belove et al column 1 lines 37-43).

As per claims 11-14, the modified Noll et al, Kaplan et al, Matyas et al, Ginter et al and Belove et al system discloses receiving said first data; examining said linking data to retrieve said second data structure; generating said first digital input based on said second data structure; regenerating said first output value based on applying said first digital input to said first integrated circuit; regenerating said first encryption key based on the regenerated first output value; and decrypting said

encrypted first data using said first encryption key (see Ginter as applied above); then first data comprises an identifier value that identifies an attribute associated with said first integrated circuit; wherein said identifier value specifies the identity of an entity into which the first integrated circuit has been incorporated; and specifies the ownership of an entity into which the first integrated circuit has been incorporated (see Belove et al column 1 lines 37-43).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

MJP

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER